PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-189543
(43)Date of publication of application : 05.07.2002

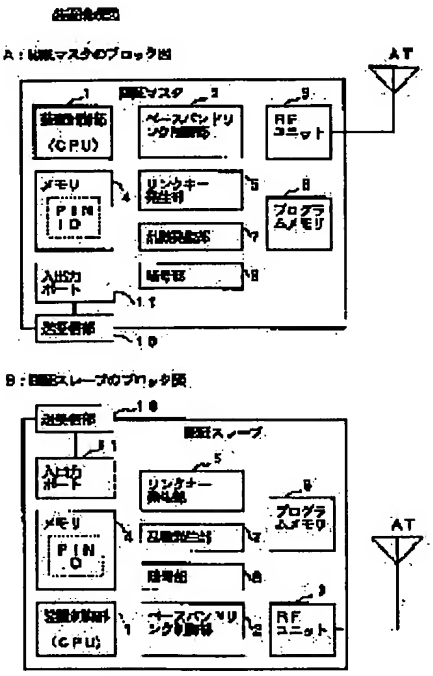
(51)Int.Cl. G06F 3/00
H04L 9/32
H04L 12/28

(21)Application number : 2000-388522
(22)Date of filing : 21.12.2000

(71)Applicant : TDK CORP
(72)Inventor : TEZUKA MASAO

(54) INFORMATION PROCESSOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an information processor capable of improving the operability of a user, and surely ensuring security by explicating a device for performing an authentication process.
SOLUTION: The information processor equipped with a radio interface having weak directivity and transmitting and receiving information with the other information processor through the radio interface having weak directivity is provided with not only the radio interface having weak directivity but also an interface having strong directivity or an adjacent type interface so that authentication identification information necessary for an authentication procedure can be acquired.



CLAIMS

[Claim(s)]
[Claim 1]In an information processor is provided with a wireless interface, and transmit and receive information by radio with other information processors via this wireless interface, An information processor provided with a directive interface for obtaining attestation identification information required in order to perform performs authentication other than said wireless interface, or an approached type interface.
[Claim 2]The information processor according to claim 1 having used said directive interface or an approached type interface, and having a function for sharing attestation identification information required for performs authentication when performing performs authentication among other information processors.
[Claim 3]The information processor according to claim 1 or 2, wherein said attestation identification information is PIN information.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention is used for the information processor which has a wireless interface.
It is related with the information processor which gave the interface for obtaining attestation identification information required for performs authentication other than said wireless interface especially.

[0002]
[Description of the Prior Art]Hereafter, a conventional example is explained based on a drawing.
[0003]**1: The equipment configuration figure of the explanation conventional example of a device is shown in drawing 3. In drawing 3, A figure is a block diagram of an attestation master, and B figure is a block diagram of an attestation slave. The device shown in drawing 3 is one example of the information processor provided with the wireless interface. And when said information processor performs performs authentication, two information processors are used, the side which attests is made into an attestation master and an attesting side is used as an attestation slave.
[0004]The Bluetooth (Bluetooth) standard can be raised as one of attestation of such an information processor, and the standards of data communications. Bluetooth (Bluetooth) is one of the protocols of wireless LAN (Local Area Network), aims at using it in very near area, and aims at the standard of a high-speed wireless LAN method at low cost. This Bluetooth is a wireless interface using the ISM (Industrial Scientific and Medical Band) belt of the 2.4GH$_Z$ belt which does not need license to a carrier frequency.
Electric wave connection area is about a maximum of 10 m.

[0005]Equip said attestation master and an attestation slave with directive weak antenna AT for transmission and reception, and to the inside. The device control part (for example, CPU) 1 which performs various control of a device, and the baseband link control part 2 which performs link control in baseband, RF unit 3 which performs control at the time of the transmission and reception in the RF (RadioFrequency : radio frequency) section, The memory (nonvolatile memory which can write in EEPROM etc. electrically) 4 which stores attestation identification information required for performs authentication, for example, PIN (Personal Identification Number) information and ID information peculiar to a device, It has the link key generating section 5 which generates the link key for cipher processing, the program memory 6 which stored the program which performs various processing in a device, the random number generation part 7 which performs generating of a random number, and the cryptopart 8 grade which performs cipher processing.
[0006]Said PIN information is information containing a number, a sign, a character, etc.
For example, it is used when the IC card itself checks that those who are going to use the IC card are just owners using this PIN information (personal identification function using PIN information).

[0007]**2: The processing flow chart of the processing explanation conventional example at the time of attestation is shown in drawing 4. Hereafter, the processing at the time of attestation is explained based on drawing 4. S1-S15 show each processing step. This processing is an example for performing authenticating processing which uses two information processors of composition of having been shown in drawing 3, makes one of these an attestation master, and is explained below by making another side into an attestation slave.
[0008]In the following processings, it is required for the memory 4 of both an attestation master and an attestation slave beforehand to store attestation identification information (for example, PIN information) and ID information by a help (user).
[0009]The following processings are processings realized when the device control part (CPU) 1 reads and executes the program of the program memory 6.
[0010]First, in an attestation master, an authentication demand is transmitted to an attestation slave (S1), then the random number generation part 7 is started, the random number for link key generations is generated, and the random number for the link key generations is transmitted to an attestation slave (S2). Then, the link key generating section 5 is started and the link key by the link key generating section 5 is made to generate using the PIN information on the memory 4 (S3). Next, the cryptopart 8 is started and the link key by the cryptopart 8 is enciphered (S4).
[0011]On the other hand, in an attestation slave, the authentication demand from an attestation master is received (S11), the random number sent from the attestation master is received (S12), the link key generating section 5 is started, and the link key by the link key generating section 5 is generated using the PIN information on the memory 4 (S13). And the cryptopart 8 is started, the link key by the cryptopart 8 is enciphered (S14), and the enciphered link key is transmitted to an attestation master (S15).
[0012]In an attestation master, if the link key from said attestation slave is received (S5), two enciphered link keys are compared (S6) and both are in agreement (collation O.K.), (S7) and this processing will be ended as an authentication success. By processing of S6, if the collated result of a link key is inharmonious, (S8) and this processing will be ended as an authentication failure.
[0013]
[Problem(s) to be Solved by the Invention]The following technical problems occurred in the above conventional things.
[0014](1) : since radio art which is represented by Bluetooth (Bluetooth) is a directive weak communication method, which devices are unclear in whether it is in an authentication process in the procedure of attestation. That is, it is not easy to specify a device selectively and to perform an authentication process clearly. Therefore, reservation of security is difficult.
[0015](2) : when performing the above authenticating processings, authenticating processing cannot be performed unless it is after setting PIN information etc. as the memory 4 of both an attestation slave and an attestation master. Therefore, before performing authenticating processing, beforehand, PIN information must be set up by a help (user), time and effort and time are taken, and it is troublesome.
[0016]An object of this invention is to raise a user's operativity, as such a conventional technical problem is solved and the device which performs the process of attestation can be specified, and to enable it to ensure reservation of security.
[0017]

[Means for Solving the Problem]This invention was constituted as follows in order to attain the aforementioned purpose.
[0018]: (1) In an information processor is provided with a wireless interface, and transmit and receive information by radio with other information processors via this wireless interface, It has a powerful directive interface for obtaining attestation identification information required in order to perform performs authentication other than said wireless interface, or an approached type interface.
[0019](2) : above (1) In an information processor, when performing performs authentication among other information processors, a powerful interface of said directivity or an approached type interface was used, and it has a function for sharing attestation identification information required for performs authentication.
[0020](3) : above (1) Or (2) In an information processor, said attestation identification information is characterized by being PIN information.
[0021](OPERATION) An information processor provided with a powerful directive interface for obtaining attestation identification information required in order to perform performs authentication other than said wireless interface, or an approached type interface is used for an attestation master and an attestation slave, and processing for obtaining attestation identification information required for performs authentication using a powerful directive interface or an approached type interface is performed.
[0022]If it does in this way, by performing a process of attestation using attestation identification information obtained by said processing, an information processor which performs a process of attestation can be specified and reservation of security can be performed certainly. Since the user can attest easily only by operation of bringing an attestation slave close to an attestation master, his operativity of a user improves.
[0023]When performing processing for obtaining attestation identification information required for performs authentication using a powerful directive interface or an approached type interface, sharing of said attestation identification information is performed automatically. Therefore, what is necessary is to hold attestation identification information only to an attestation master, and time and effort of YUSA is not taken and it is not necessary to also carry out troublesome operation also at this point.
[0024]
[Embodiment of the Invention]Hereafter, an embodiment of the invention is described in detail based on a drawing.
[0025]**1: The illustration device lineblock diagram of a device is shown in drawing 1. In drawing 1, A figure is a block diagram of an attestation master, and B figure is a block diagram of an attestation slave. This device adds the interface for newly obtaining attestation identification information required for performs authentication to the conventional information processor (an attestation master and an attestation slave) shown in drawing 3.
[0026]Namely, to the attestation master and attestation slave which were shown in drawing 1. Besides a directive weak wireless interface like Bluetooth (Bluetooth) explained by said conventional example, The interface which specifies a device selectively and can attest it clearly and which had directivity strongly, and an approached type interface are given, and it enables it to make a user conscious of an authentication process by dialing operation.
[0027]In order to make a user conscious of an authentication process and to carry out dialing operation to him, It is desirable for the angle in which the range of a signal is less than several meters, and a signal is detected by the device and it deals to be less than 50 degrees, and infrared rays or optical interfaces, such as IrDA (Infrared Data Association) and a bar code scanner, can be used.
[0028]Or if it approaches more and is in less than about 20 cm, the purpose which specifies a device as a user selectively and can be attested clearly can also be attained, In this case, the distance of 2 mm or the about 20-cm approached type interface provided in the standard of "ISO/IEC10536" and "ISO/IEC14443" can also be used.
[0029]Although said IrDA is the organization established for the purpose of standard establishment of infrared ray data communication, generally it points out the telecommunications standard which IrDA defined in many cases. There are IrDA1.0 and IrDA1.1 as main standards used with a personal computer.
[0030]In "ISO/IEC10536" of the interface of said approached type, the distance of an attestation master and an attestation slave can approach to about 2 mm, and, above "ISO/IEC14443", can approach to about 20 cm. Hereafter, it explains concretely.
[0031]In this example, as shown in drawing 1, between two information processors, either is made into an attestation master and authenticating processing is performed by making the device of the other into an attestation slave. In these information processors (an attestation master and an attestation slave). Have directive weak antenna AT for transmission and reception, and to the inside. The device control part (for example, CPU) 1 which performs various control of a device, and the baseband link control part 2 which performs link control in baseband, RF unit 3 which performs transmit/receive control in RF belt, and the memory (nonvolatile memory which can write in EEPROM etc. electrically) 4 which stores PIN information (attestation identification information required for performs authentication), and ID information peculiar to a device, The link key generating section 5 for generating the link key in cipher processing, It has the input/output port 11 grade which performs the program memory 6 which stored the program for performing various processing in a device, the random number generation part 7 which generates a random number, the cryptopart 8 which performs cipher processing, the strong directive transmission and reception section 10, and radial transfer of transmission and reception signals.
[0032]In this case, the portion containing antenna AT and RF unit 3 is a directive weak wireless interface, and a portion including the transmission and reception section 10 and the input/output port 11 is a powerful directive interface or an approached type interface.
[0033]**2: The sharing processing flow chart of the explanation PIN information on sharing processing of PIN information is shown in drawing 2. Hereafter, sharing processing of PIN information is explained based on drawing 2. S21-S33 of drawing 2 show each processing step.
[0034]Before beginning the following processings, PIN information shall not be stored in the memory 4 of an attestation slave, but PIN information shall be stored only in the memory 4 of an attestation master.
[0035]And the PIN information stored in the memory 4 of an attestation master is sent to an attestation slave, and it enables it to store PIN information in the memory 4 of an attestation slave by sharing processing of the following PIN information. Hereafter, it explains in detail.
[0036]First, an attestation slave publishes the signal for [detecting] (S31), and transmits to an attestation master. If the signal for [waiting and this detecting] is detected for detection of the signal for [detecting-from said attestation slave] (S21), an attestation master will transmit the demand of ID (identification information peculiar to a device) to an attestation slave (S22), and will perform receiving waiting of ID (S23).
[0037]If the demand of ID from an attestation master is received, an attestation slave will take out ID demanded from the memory 4, and will transmit to an attestation master (S32). It is judged whether when ID from an attestation slave was received (S24), the attestation master took out ID stored in the memory 4, compared the ID and said ID which received, and both corresponded (S25).
[0038]As a result, if both are in agreement, suppose that ID has been checked (S26). If ID is checked as mentioned above, PIN information is taken out from the memory 4 and it transmits to an attestation slave (S27). By processing of S25, processing is ended as it is noting that the check of ID cannot be performed, when both are inharmonious.
[0039]Then, if the PIN information from an attestation master is received (S33), an attestation slave will store that PIN information in the memory 4, and will end this processing. Thus, the PIN information which an attestation master holds is sent to an attestation slave, and sharing of PIN information can be attained by making PIN information hold to an attestation slave.
[0040]Processing of the conventional example shown in drawing 4 by sharing of the aforementioned PIN information using the PIN information

since PIN information is storable in the memory 4 of both an attestation master and an attestation slave performs authenticating processing.
[0041]Although said PIN information is attestation identification information required for performs authentication, said not only PIN information but other arbitrary identification information can be used for this attestation identification information.
[0042]**3: Other explanation (1) : In sharing processing of the PIN information shown in drawing 2, since PIN information is stored in memories, such as EEPROM, Although what is necessary is just to carry out to wireless LAN, such as Bluetooth (Bluetooth) shown in drawing 4, once before the processing of a flow chart which makes attestation connection, whenever it connects with wireless LAN depending on the case, it is good in a line each time. Naturally sharing processing is needed for connecting with the wireless LAN which needs different PIN information.
[0043]: (2) As an example of said information processor, A personal computer, PDA (Personal Digital Assistant), A workstation, a router, a printer, a headset, a digital camera, A hard disk drive, a removable disk device, VTR, TV, an air-conditioner (air-conditioner), a refrigerator, voice recording playback equipment (a tape recorder, IC recorder, etc.), a remote control, a car, a vending machine, a microwave oven, telephone, etc. can be considered.
[0044]
[Effect of the Invention]As explained above, according to this invention, there are the following effects.
[0045]The powerful directive interface for obtaining attestation identification information required in order to perform performs authentication other than said wireless interface, Or the information processor provided with the approached type interface is used for an attestation master and an attestation slave, and processing for obtaining attestation identification information required in order to perform performs authentication using a powerful directive interface or an approached type interface is performed.
[0046]If it does in this way, by performing the process of attestation using the attestation identification information obtained by said processing, the information processor which performs the process of attestation can be specified and reservation of security can be performed certainly. Since the user can attest easily only by operation of bringing an attestation slave close to an attestation master, his operativity of a user improves.
[0047]When performing processing for obtaining said attestation identification information using a powerful directive interface or an approached type interface, sharing of said attestation identification information is performed automatically. Therefore, what is necessary is to hold attestation identification information only to the attestation master, and time and effort is not taken and it is not necessary to also carry out troublesome operation also at this point.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is an equipment configuration figure in an embodiment of the invention, and A figure is a block diagram of an attestation master, and B figure is a block diagram of an attestation slave.
[Drawing 2]It is a sharing processing flow chart of the PIN information in an embodiment of the invention.
[Drawing 3]It is an equipment configuration figure of a conventional example, and A figure is a block diagram of an attestation master, and B figure is a block diagram of an attestation slave.
[Drawing 4]It is a processing flow chart of a conventional example.
[Description of Notations]
1 Device control part
2 Baseband link control part
3 RF unit
4 Memory
5 Link key generating section
6 Program memory
7 Random number generation part
8 Cryptopart
10 Transmission and reception section
11 Input/output port

[Translation done.]

* NOTICES *

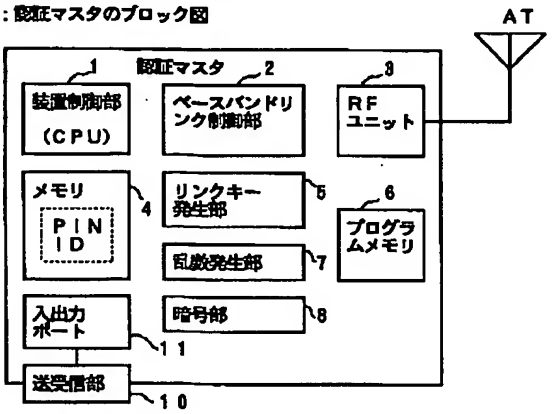
JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

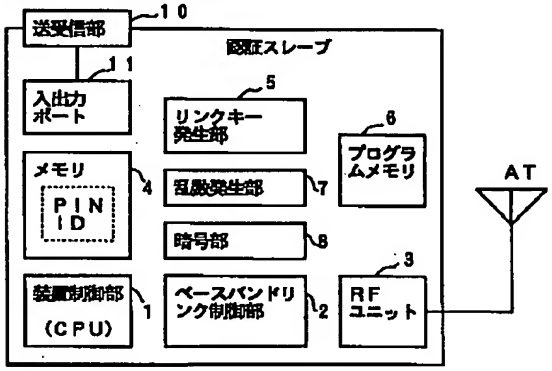
DRAWINGS

[Drawing 1]
装置構成図

A：認証マスタのブロック図

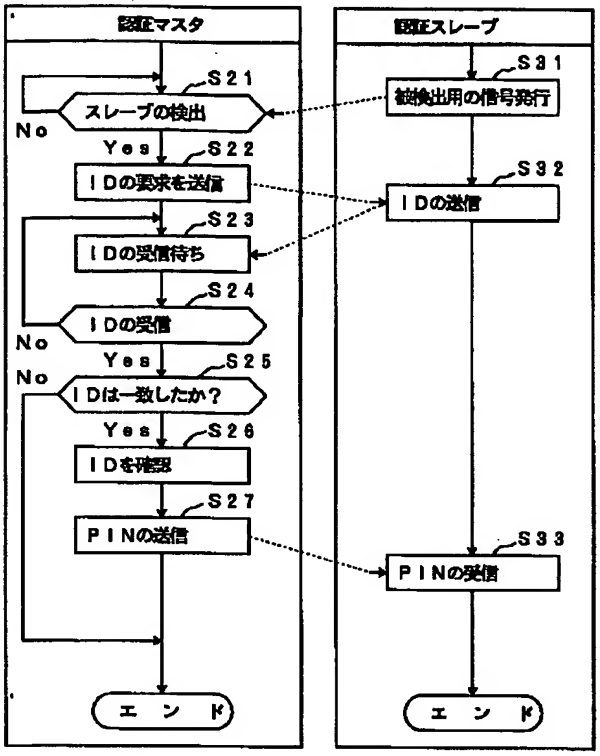


B：認証スレーブのブロック図



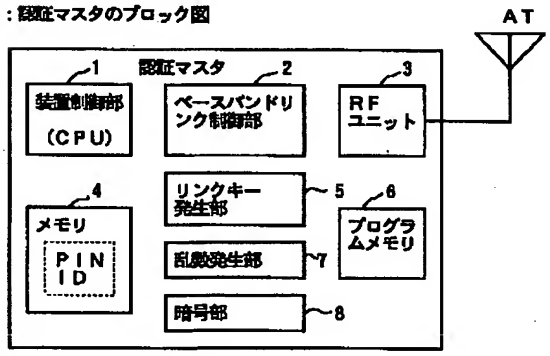
[Drawing 2]

ＰＩＮ情報の共有化処理フローチャート

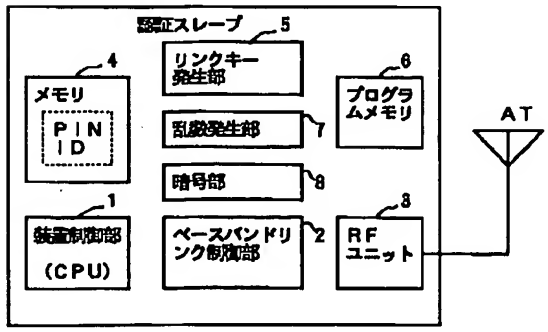


[Drawing 3]
従来例の装置構成図

Ａ：認証マスタのブロック図

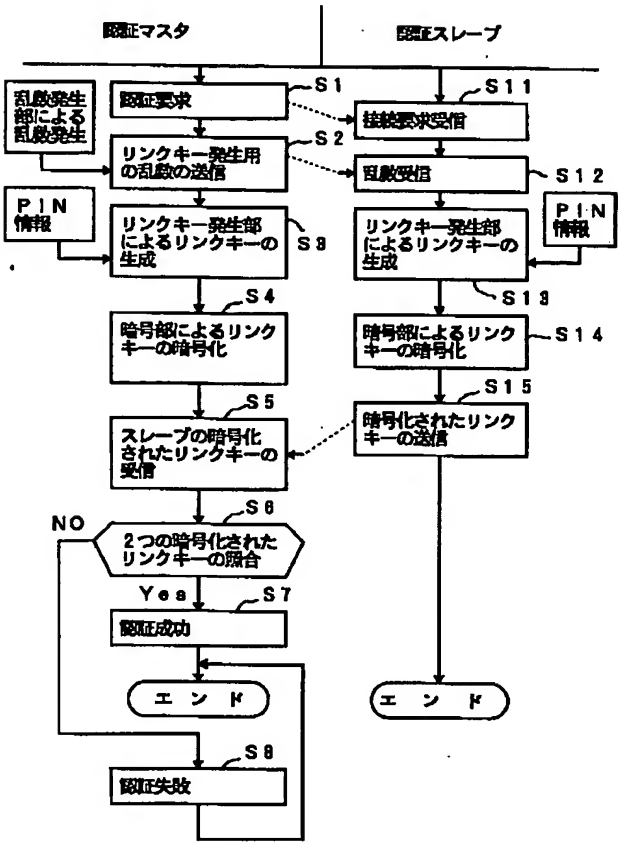


Ｂ：認証スレーブのブロック図



[Drawing 4]

従来例の処理フローチャート



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－189543
（P2002－189543A）
(43)公開日　平成14年７月５日(2002.7.5)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード*(参考)
Ｇ０６Ｆ　3/00		Ｇ０６Ｆ　3/00	Ｃ	５Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　12/28	３００Ｚ	５Ｋ０３３
12/28	３００	9/00	６７３Ｂ	

審査請求　未請求　請求項の数３　ＯＬ　（全 6 頁）

(21)出願番号　特願2000－388522(P2000－388522)

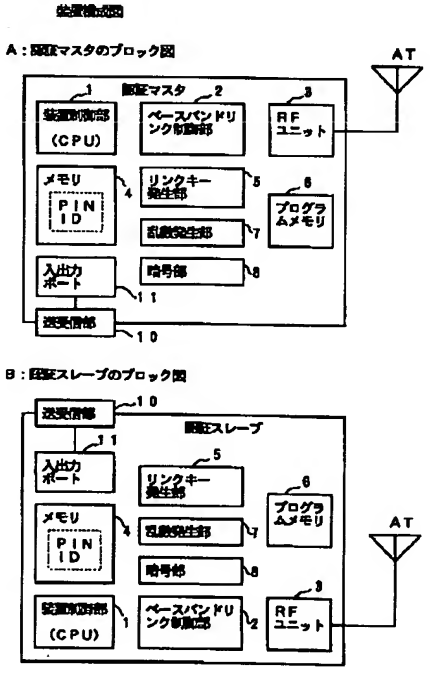
(22)出願日　平成12年12月21日(2000.12.21)

(71)出願人　000003067
ティーディーケイ株式会社
東京都中央区日本橋１丁目13番１号
(72)発明者　手塚　正男
東京都中央区日本橋一丁目13番１号　ティーディーケイ株式会社内
(74)代理人　100096530
弁理士　今村　辰夫　（外２名）

Ｆターム(参考)　5J104 AA07 KA01 KA02 NA05 PA01
5K033 AA08 DA01 DA17

(54)【発明の名称】　情報処理装置

(57)【要約】
【課題】本発明は情報処理装置に関し、認証のプロセスを行う装置を明示できるようにして、ユーザの操作性を向上させ、かつ、セキュリティの確保が確実に行えるようにする。
【解決手段】指向性の弱い無線インタフェースを備え、該指向性の弱い無線インタフェースを介して他の情報処理装置と情報の送受信を行う情報処理装置において、前記指向性の弱い無線インタフェースの他に、認証手続きに必要な認証識別情報を得るための指向性の強いインタフェース、又は近接型のインタフェースを備えた。



1

【特許請求の範囲】
【請求項１】無線インタフェースを備え、該無線インタフェースを介して他の情報処理装置との無線通信により情報の送受信を行う情報処理装置において、
前記無線インタフェースの他に、認証手続きを行うために必要な認証識別情報を得るための指向性のインタフェース、又は近接型のインタフェースを備えていることを特徴とする情報処理装置。
【請求項２】他の情報処理装置との間で認証手続きを行う際に、前記指向性のインタフェース、又は近接型のインタフェースを使用して、認証手続きに必要な認証識別情報を共有するための機能を備えていることを特徴とする請求項１記載の情報処理装置。
【請求項３】前記認証識別情報はＰＩＮ情報であることを特徴とする請求項１又は２記載の情報処理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、無線インタフェースを有する情報処理装置に利用されるものであり、特に、前記無線インタフェースの他に、認証手続きに必要な認証識別情報を得るためのインタフェースを持たせた情報処理装置に関する。
【０００２】
【従来の技術】以下、図面に基づいて従来例を説明する。
【０００３】§１：装置の説明
従来例の装置構成図を図３に示す。図３において、Ａ図は認証マスタのブロック図、Ｂ図は認証スレーブのブロック図である。図３に示す装置は、無線インタフェースを備えた情報処理装置の１例である。そして、前記情報処理装置により認証手続きを行う場合には、２台の情報処理装置を使用し、認証を行う側を認証マスタとし、被認証側を認証スレーブとして使用する。
【０００４】このような情報処理装置の認証及びデータ伝送の規格の一つとして、ブルートゥース（Bluetooth）規格を上げることができる。なお、ブルートゥース（Bluetooth）は無線ＬＡＮ（Local Area Network）のプロトコルの一つであり、極めて近いエリアで使用することを目的としており、ローコストで高速な無線ＬＡＮ方式の標準を狙ったものである。また、このブルートゥースは、免許が不要な２．４ＧＨｚ帯のＩＳＭ（Industrial Scientific and Medical Band）帯を搬送周波数に使う無線インタフェースであり、電波接続エリアは最大１０ｍ程度である。
【０００５】前記認証マスタ及び認証スレーブには、指向性の弱い送受信用のアンテナＡＴを備えると共に、その内部には、装置の各種制御を行う装置制御部（例えば、ＣＰＵ）１と、ベースバンドでのリンク制御を行うベースバンドリンク制御部２と、ＲＦ（Radio Frequency：無線周波数）部における送受信時の制御を行うＲＦ

2

ユニット３と、認証手続きに必要な認証識別情報、例えば、ＰＩＮ（Personal Identification Number）情報や装置固有のＩＤ情報を格納しておくメモリ（ＥＥＰＲＯＭ等の電気的に書き込み可能な不揮発性メモリ）４と、暗号処理用のリンクキーを発生させるリンクキー発生部５と、装置内の各種処理を行うプログラムを格納したプログラムメモリ６と、乱数の発生を行う乱数発生部７と、暗号処理を行う暗号部８等を備えている。
【０００６】なお、前記ＰＩＮ情報は、数字、記号、文字等を含む情報であり、例えば、ＩＣカードを使用しようとしている人が正当な持ち主であることを、該ＰＩＮ情報を用いてＩＣカード自身が確認する場合（ＰＩＮ情報を用いた本人確認機能）等に使用されるものである。
【０００７】§２：認証時の処理説明
従来例の処理フローチャートを図４に示す。以下、図４に基づいて認証時の処理を説明する。なお、Ｓ１～Ｓ１５は各処理ステップを示す。この処理は、図３に示した構成の情報処理装置を２台使用し、その一方を認証マスタとし、他方を認証スレーブとして以下に説明する認証処理を行う例である。
【０００８】以下の処理では、予め、認証マスタと認証スレーブの両方のメモリ４に、人手（ユーザ）により認証識別情報（例えば、ＰＩＮ情報）とＩＤ情報を格納しておくことが必要である。
【０００９】また、以下の処理は、装置制御部（ＣＰＵ）１がプログラムメモリ６のプログラムを読み出して実行することにより実現する処理である。
【００１０】先ず、認証マスタでは、認証スレーブに対して認証要求を送信し（Ｓ１）、続いて、乱数発生部７を起動してリンクキー発生用の乱数を発生させ、そのリンクキー発生用の乱数を認証スレーブへ送信する（Ｓ２）。その後、リンクキー発生部５を起動し、メモリ４のＰＩＮ情報を用いてリンクキー発生部５によるリンクキーを生成させる（Ｓ３）。次に、暗号部８を起動して、暗号部８によるリンクキーの暗号化を行う（Ｓ４）。
【００１１】一方、認証スレーブでは、認証マスタからの認証要求を受信し（Ｓ１１）、認証マスタから送られてきた乱数を受信し（Ｓ１２）、リンクキー発生部５を起動し、メモリ４のＰＩＮ情報を用いてリンクキー発生部５によるリンクキーを生成する（Ｓ１３）。そして、暗号部８を起動して、暗号部８によるリンクキーの暗号化を行い（Ｓ１４）、暗号化されたリンクキーを認証マスタへ送信する（Ｓ１５）。
【００１２】認証マスタでは、前記認証スレーブからのリンクキーを受信すると（Ｓ５）、２つの暗号化されたリンクキーの照合を行い（Ｓ６）、両者が一致すれば（照合ＯＫ）、認証成功として（Ｓ７）、この処理を終了する。また、Ｓ６の処理で、リンクキーの照合結果が不一致であれば、認証失敗として（Ｓ８）、この処理を

終了する。

【００１３】

【発明が解決しようとする課題】前記のような従来のものにおいては、次のような課題があった。

【００１４】(1)：ブルートゥース（Bluetooth）に代表されるような無線技術は、指向性の弱い通信方式であるため、認証の手続き中に、どの装置同士が認証プロセスにあるのか分かり難い。すなわち、装置を選択的に指定して明示的に認証プロセスを行うことが容易でない。そのため、セキュリティの確保が難しい。

【００１５】(2)：前記のような認証処理を行う場合、認証スレーブと認証マスタの両方のメモリ４にＰＩＮ情報等を設定してからでないと認証処理を行うことはできない。そのため、認証処理を行う前に、予め、人手（ユーザ）によりＰＩＮ情報の設定をしなければならず、手間や時間がかかり、面倒である。

【００１６】本発明は、このような従来の課題を解決し、認証のプロセスを行う装置を明示できるようにして、ユーザの操作性を向上させ、かつ、セキュリティの確保が確実に行えるようにすることを目的とする。

【００１７】

【課題を解決するための手段】本発明は前記の目的を達成するため、次のように構成した。

【００１８】(1)：無線インタフェースを備え、該無線インタフェースを介して他の情報処理装置との無線通信により情報の送受信を行う情報処理装置において、前記無線インタフェースの他に、認証手続きを行うために必要な認証識別情報を得るための指向性の強いインタフェース、又は近接型のインタフェースを備えていることを特徴とする。

【００１９】(2)：前記(1)の情報処理装置において、他の情報処理装置との間で認証手続きを行う際に、前記指向性の強いインタフェース、又は近接型のインタフェースを使用して、認証手続きに必要な認証識別情報を共有するための機能を備えていることを特徴とする。

【００２０】(3)：前記(1)又は(2)の情報処理装置において、前記認証識別情報はＰＩＮ情報であることを特徴とする。

【００２１】（作用）前記無線インタフェースの他に、認証手続きを行うために必要な認証識別情報を得るための指向性の強いインタフェース、又は近接型のインタフェースを備えた情報処理装置を認証マスタ及び認証スレーブに使い、指向性の強いインタフェース、又は近接型のインタフェースを利用して認証手続きに必要な認証識別情報を得るための処理を行う。

【００２２】このようにすれば、前記処理で得られた認証識別情報を使用して認証のプロセスを行うことにより、認証のプロセスを行う情報処理装置を明示することができセキュリティの確保が確実にできる。また、ユーザは、認証スレーブを認証マスタに近づけるだけの操作で簡単に認証を行うことができるから、ユーザの操作性が向上する。

【００２３】また、指向性の強いインタフェース、又は近接型のインタフェースを使用して認証手続きに必要な認証識別情報を得るための処理を行う際、前記認証識別情報の共有化が自動的に行われる。従って、認証マスタにだけ認証識別情報を保持しておけば良く、この点でもユーザの手間がかからず、面倒な操作もしなくて済む。

【００２４】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて詳細に説明する。

【００２５】§１：装置の説明

装置構成図を図１に示す。図１において、Ａ図は認証マスタのブロック図、Ｂ図は認証スレーブのブロック図である。この装置は、図３に示した従来の情報処理装置（認証マスタ及び認証スレーブ）に、新たに認証手続きに必要な認証識別情報を得るためのインタフェースを追加したものである。

【００２６】すなわち、図１に示した認証マスタと認証スレーブには、前記従来例で説明したブルートゥース（Bluetooth）のような指向性の弱い無線インタフェースの他に、装置を選択的に指定して明示的に認証できる、指向性を強く持ったインタフェースや近接型のインタフェースを持たせ、接続操作によりユーザに認証プロセスを意識させることができるようにしたものである。

【００２７】ユーザに認証プロセスを意識させて接続操作するためには、信号の到達距離が数ｍ以内でかつ信号が装置に感知されうる角度が５０度以内であることが望ましく、ＩｒＤＡ（Infrared Data Association）やバーコードスキャナなどの赤外線あるいは光学的インタフェースを用いることができる。

【００２８】或いは、より近接して２０ｃｍ程度以内にあれば、ユーザに装置を選択的に指定して明示的に認証できる目的を達することもでき、この場合には「ＩＳＯ／ＩＥＣ１０５３６」「ＩＳＯ／ＩＥＣ１４４４３」の規格に定められた、距離２ｍｍ若しくは２０ｃｍ程度の近接型インタフェースを用いることもできる。

【００２９】なお、前記ＩｒＤＡは、赤外線データ通信の規格制定を目的として設立された団体であるが、一般には、ＩｒＤＡが定めた通信規格を指すことが多い。パーソナルコンピュータで利用される主な規格として、ＩｒＤＡ１．０、及びＩｒＤＡ１．１がある。

【００３０】また、前記近接型のインタフェースの「ＩＳＯ／ＩＥＣ１０５３６」では、認証マスタと認証スレーブとの距離は２ｍｍ程度まで接近でき、前記「ＩＳＯ／ＩＥＣ１４４４３」では２０ｃｍ程度まで接近できる。以下、具体的に説明する。

【００３１】この例では図１に示したように、２つの情報処理装置間では、何れか一方を認証マスタとし、他方の装置を認証スレーブとして認証処理を行う。これらの

情報処理装置（認証マスタ及び認証スレーブ）には、送受信用の指向性の弱いアンテナＡＴを備えると共に、その内部には、装置の各種制御を行う装置制御部（例えば、ＣＰＵ）１と、ベースバンドでのリンク制御を行うベースバンドリンク制御部２と、ＲＦ帯での送受信制御を行うＲＦユニット３と、ＰＩＮ情報（認証手続きに必要な認証識別情報）や装置固有のＩＤ情報を格納しておくメモリ（ＥＥＰＲＯＭ等の電気的に書き込み可能な不揮発性メモリ）４と、暗号処理でのリンクキーを発生させるためのリンクキー発生部５と、装置内の各種処理を行うためのプログラムを格納したプログラムメモリ６と、乱数を発生させる乱数発生部７と、暗号処理を行う暗号部８と、指向性の強い送受信部１０と、送受信信号の入出力処理を行う入出力ポート１１等を備えている。

【００３２】この場合、アンテナＡＴ、ＲＦユニット３を含む部分が指向性の弱い無線インタフェースであり、送受信部１０と入出力ポート１１を含む部分が指向性の強いインタフェース、又は近接型のインタフェースである。

【００３３】§２：ＰＩＮ情報の共有化処理の説明

ＰＩＮ情報の共有化処理フローチャートを図２に示す。以下、図２に基づいてＰＩＮ情報の共有化処理を説明する。なお、図２のＳ２１～Ｓ３３は各処理ステップを示す。

【００３４】以下の処理を始める前には、認証スレーブのメモリ４にはＰＩＮ情報が格納されておらず、認証マスタのメモリ４にのみＰＩＮ情報が格納されているものとする。

【００３５】そして、以下のＰＩＮ情報の共有化処理により、認証マスタのメモリ４に格納されているＰＩＮ情報を認証スレーブへ送り、認証スレーブのメモリ４にＰＩＮ情報を格納できるようにする。以下、詳細に説明する。

【００３６】先ず、認証スレーブは、被検出用の信号を発行し（Ｓ３１）、認証マスタへ送信する。認証マスタは前記認証スレーブからの被検出用の信号の検出を待ち、該被検出用の信号を検出すると（Ｓ２１）、認証スレーブに対してＩＤ（装置固有の識別情報）の要求を送信し（Ｓ２２）、ＩＤの受信待ちを行う（Ｓ２３）。

【００３７】認証スレーブは認証マスタからのＩＤの要求を受信すると、メモリ４から要求されたＩＤを取り出し、認証マスタへ送信する（Ｓ３２）。認証マスタは認証スレーブからのＩＤを受信すると（Ｓ２４）、メモリ４に格納されているＩＤを取り出し、そのＩＤと前記受信したＩＤとを比較し、両者が一致したか否かを判断する（Ｓ２５）。

【００３８】その結果、両者が一致したらＩＤを確認できたとする（Ｓ２６）。前記のようにしてＩＤが確認できたら、メモリ４からＰＩＮ情報を取り出し認証スレーブへ送信する（Ｓ２７）。また、Ｓ２５の処理で、両者が不一致の場合は、ＩＤの確認ができなかったとして、そのまま処理を終了する。

【００３９】その後、認証スレーブは、認証マスタからのＰＩＮ情報を受信すると（Ｓ３３）、そのＰＩＮ情報をメモリ４に格納してこの処理を終了する。このようにして、認証マスタが保持するＰＩＮ情報を認証スレーブへ送り、認証スレーブにＰＩＮ情報を保持させることでＰＩＮ情報の共有化を達成できる。

【００４０】前記のＰＩＮ情報の共有化により、認証マスタと認証スレーブの両方のメモリ４にＰＩＮ情報が格納できるので、そのＰＩＮ情報を用いて、図４に示す従来例の処理により認証処理を行う。

【００４１】なお、前記ＰＩＮ情報は認証手続きのために必要な認証識別情報であるが、この認証識別情報は、前記ＰＩＮ情報に限らず、他の任意の識別情報を用いることができる。

【００４２】§３：その他の説明

(1)：図２に示したＰＩＮ情報の共有化処理において、ＰＩＮ情報はＥＥＰＲＯＭ等のメモリに格納されるので、図４に示すブルートゥース（Bluetooth）等の無線ＬＡＮに認証接続するフローチャートの処理の前に、１回行えば良いが、場合によっては無線ＬＡＮに接続する毎に毎回行っても良い。異なったＰＩＮ情報が必要な無線ＬＡＮに接続するには当然共有化処理は必要となる。

【００４３】(2)：前記情報処理装置の具体例としては、パーソナルコンピュータ、ＰＤＡ（Personal Digital Assistant）、ワークステーション、ルータ、プリンタ、ヘッドセット、ディジタルカメラ、ハードディスク装置、リムーバブルディスク装置、ＶＴＲ、ＴＶ、エアコン（空調装置）、冷蔵庫、音声記録再生装置（テープレコーダ、ＩＣレコーダ等）、リモコン、自動車、自動販売機、電子レンジ、電話機等が考えられる。

【００４４】

【発明の効果】以上説明したように、本発明によれば次のような効果がある。

【００４５】前記無線インタフェースの他に、認証手続きを行うために必要な認証識別情報を得るための指向性の強いインタフェース、又は近接型のインタフェースを備えた情報処理装置を認証マスタ及び認証スレーブに使い、指向性の強いインタフェース、又は近接型のインタフェースを利用して認証手続きを行うために必要な認証識別情報を得るための処理を行う。

【００４６】このようにすれば、前記処理で得られた認証識別情報を使用して認証のプロセスを行うことにより、認証のプロセスを行う情報処理装置を明示することができセキュリティの確保が確実にできる。また、ユーザは、認証スレーブを認証マスタに近づけるだけの操作で簡単に認証を行うことができるから、ユーザの操作性が向上する。

【００４７】また、指向性の強いインタフェース、又は

近接型のインタフェースを使用して前記認証識別情報を得るための処理を行う際、前記認証識別情報の共有化が自動的に行われる。従って、認証マスタにだけ認証識別情報を保持しておけば良く、この点でも手間がかからず、面倒な操作もしなくて済む。

【図面の簡単な説明】

【図１】本発明の実施の形態における装置構成図であり、Ａ図は認証マスタのブロック図、Ｂ図は認証スレーブのブロック図である。

【図２】本発明の実施の形態におけるＰＩＮ情報の共有化処理フローチャートである。

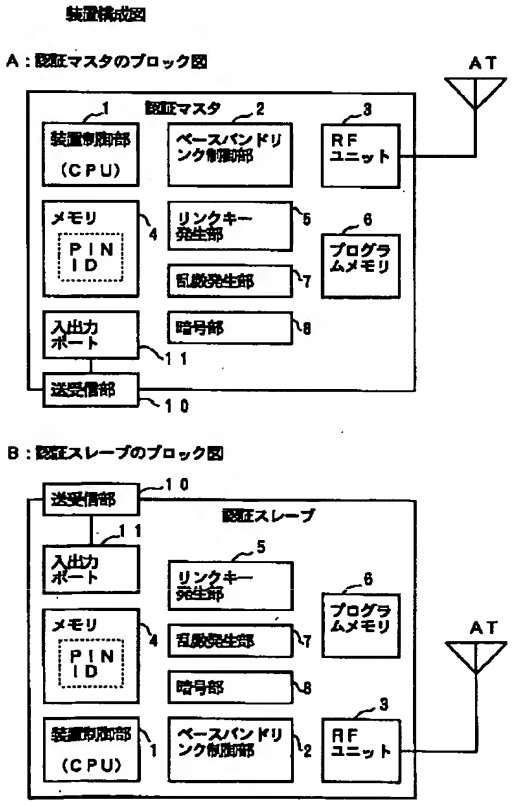
【図３】従来例の装置構成図であり、Ａ図は認証マスタのブロック図、Ｂ図は認証スレーブのブロック図である。

【図４】従来例の処理フローチャートである。

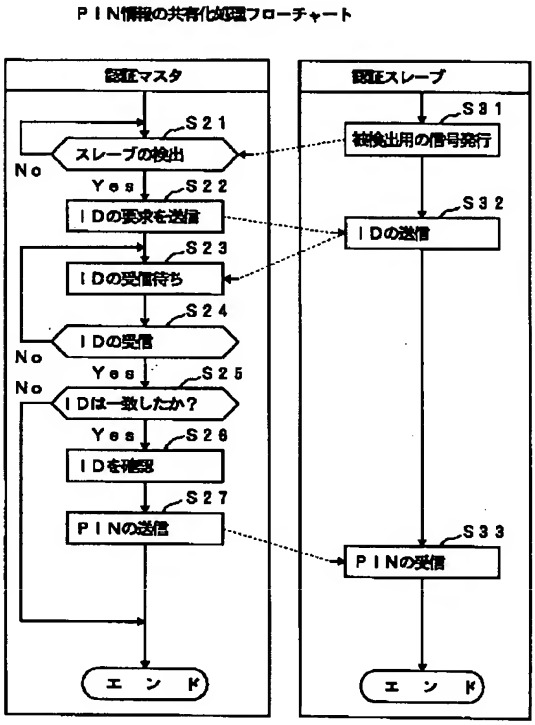
【符号の説明】

1　装置制御部
2　ベースバンドリンク制御部
3　ＲＦユニット
4　メモリ
5　リンクキー発生部
6　プログラムメモリ
7　乱数発生部
8　暗号部
１０　送受信部
１１　入出力ポート

【図１】



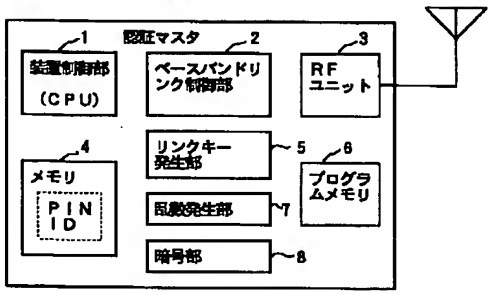
【図２】



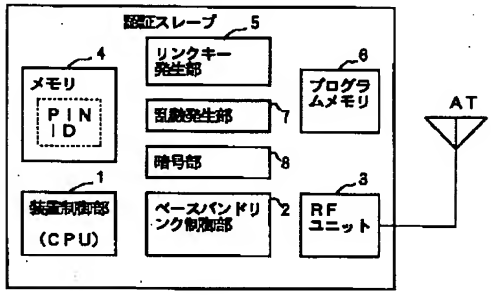
【図３】

従来例の装置構成図

A：認証マスタのブロック図



B：認証スレーブのブロック図



【図４】

従来例の処理フローチャート